

(b) *Significant interagency support requirements.* Agency heads must ensure that a Memorandum of Agreement/Understanding is established for each SAP that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

§ 2001.50 Telecommunications automated information systems and network security.

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation*.

§ 2001.51 Technical security.

Based upon the risk management factors referenced in § 2001.40 of this directive, agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, *TEMPEST Countermeasures for Facilities*, and SPB Issuance 6-97, *National Policy on Technical Surveillance Countermeasures*.

§ 2001.52 Emergency authority.

(a) Agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations.

(b) In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

(1) Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

(2) Limit the number of individuals who receive it;

(3) Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in § 2001.46, or other means deemed necessary when time is of the essence;

(4) Provide instructions about what specific information is classified and how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement;

(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

(i) A description of the disclosed information;

(ii) To whom the information was disclosed;

(iii) How the information was disclosed and transmitted;

(iv) Reason for the emergency release;

(v) How the information is being safeguarded; and

(vi) A description of the briefings provided and a copy of the nondisclosure agreements signed.

(7) Information disclosed in emergency situations shall not be required to be declassified as a result of such disclosure or subsequent use by a recipient.

§ 2001.53 Open storage areas.

This section describes the minimum construction standards for open storage areas.

(a) *Construction.* The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in